

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-003256

(43)Date of publication of application : 06.01.1998

(51)Int.Cl. G09C 1/00
G09C 1/00
G09C 1/00
G11B 20/10
H04L 9/08
H04L 9/06
H04L 9/14

(21)Application number : 08-269502

(71)Applicant : SONY CORP

(22)Date of filing : 11.10.1996

(72)Inventor : ISHIGURO RYUJI

(30)Priority

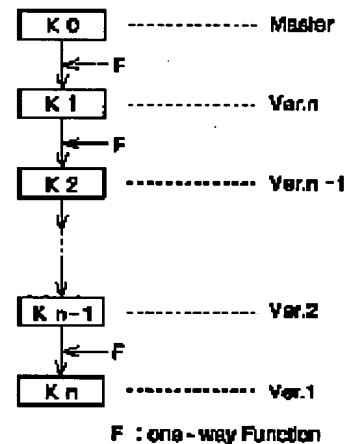
Priority number : 07267249	Priority date : 16.10.1995	Priority country : JP
07267250	16.10.1995	JP
08 93800	16.04.1996	JP

(54) CIPHERING METHOD AND DEVICE THEREFOR, RECORDING METHOD, DECODING METHOD AND DEVICE THEREFOR AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To easily control the ciphering key.

SOLUTION: A ciphering key K1 is generated from a master key K0 using a unidirectional function, a next ciphering key K2 is generated from the key K1 using the function and similarly n-hierarchical ciphering keys K1 to Kn are generated. Then, information is ciphered by the key Kn and the information is decoded by the ciphering key Kn. If the key Kn is read, the information is ciphered by the key Kn-1 and the information is decoded by the key Kn-1. Thus, the information, which is ciphered by the key Kn, is decoded by the key Kn obtained from the key Kn-1 using the function and the user is only required to maintain the latest key Kn-1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-3256

(43) 公開日 平成10年(1998) 1月6日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 A
	6 1 0	7259-5 J		6 1 0 B
	6 6 0	7259-5 J		6 6 0 D
		7259-5 J		6 6 0 E
G 1 1 B 20/10		7736-5 D	G 1 1 B 20/10	H
審査請求 未請求 請求項の数28 O L (全 13 頁) 最終頁に続く				

(21) 出願番号 特願平8-269502

(22) 出願日 平成8年(1996)10月11日

(31) 優先権主張番号 特願平7-267249

(32) 優先日 平7(1995)10月16日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平7-267250

(32) 優先日 平7(1995)10月16日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平8-93800

(32) 優先日 平8(1996)4月16日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 石黒 隆二

東京都品川区北品川6丁目7番35号 ソニー株式会社内

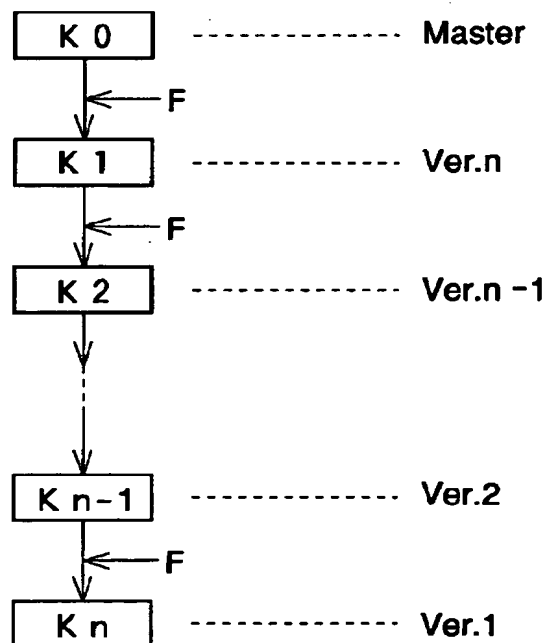
(74) 代理人 弁理士 稲本 義雄

(54) 【発明の名称】 暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録媒体

(57) 【要約】

【課題】 暗号化キーの管理を容易にする。

【解決手段】 マスタキーK0から一方向関数を用いて暗号化キーK1を作成し、暗号化キーK1から一方向関数を用いて次の暗号化キーK2を作成し、同様にしてn階層の暗号化キーK1乃至Knを作成する。暗号化キーKnにより情報を暗号化し、この情報を暗号化キーKnで復号化する。暗号化キーKnが解読された場合、暗号化キーKn-1を用いて情報を暗号化し、この情報を暗号化キーKn-1で復号化する。暗号化キーKnで暗号化された情報は、暗号化キーKn-1から一方向関数を用いて求めた暗号化キーKnで復号化することができ、ユーザは最新の暗号化キーKn-1だけを保持すればよい。



F : one-way Function

【特許請求の範囲】

【請求項1】 所定の情報を所定の暗号化キーを用いて暗号化する暗号化方法において、

上記暗号化キーを一方向関数を用いて階層化し、
上記階層化された暗号化キーを用いて上記所定の情報を暗号化することを特徴とする暗号化方法。

【請求項2】 階層化された上記暗号化キーのうち、階層化するときの最初の暗号化キーは、マスターキーであることを特徴とする請求項1に記載の暗号化方法。

【請求項3】 上記階層化された暗号化キーを用いて特定情報を暗号化することを特徴とする請求項1に記載の暗号化方法。

【請求項4】 暗号化された所定の情報を記録媒体に記録する記録方法において、

一方向関数を用いて階層化された暗号化キーを用いて暗号化された所定の情報を受信し、
上記暗号化された所定の情報を上記記録媒体に記録することを特徴とする記録方法。

【請求項5】 上記暗号化キーを用いて暗号化された特定情報を受信し、
上記暗号化された所定の情報とともに上記暗号化された特定情報を上記記録媒体に記録することを特徴とする請求項4に記載の記録方法。

【請求項6】 暗号化された所定の情報を復号化する復号化方法において、

暗号化された所定の情報を受信し、
一方向関数を用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化することを特徴とする復号化方法。

【請求項7】 階層化された上記暗号化キーのうち、階層化するときの最初の暗号化キーは、マスターキーであり、
一方向関数を用いて上記マスターキーから暗号化キーに対応する復号化キーを生成することを特徴とする請求項6に記載の復号化方法。

【請求項8】 暗号化された特定情報を受信し、
暗号化されていない上記特定情報、暗号化された上記特定情報及び上記復号化キーを決定するための情報から上記復号化キーを決定し、
その決定された復号化キーを用いて上記暗号化された所定の情報を復号化することを特徴とする請求項6に記載の復号化方法。

【請求項9】 上記復号化キーを決定するための上記情報は、マスターキー、もしくは最新の暗号化キーの情報であることを特徴とする請求項8に記載の復号化方法。

【請求項10】 上記復号化キーは、
上記復号化キーを決定するための上記情報を用いて、上記暗号化された特定情報を復号化するステップと、
その復号化された特定情報と暗号化されていない上記特定情報とを比較し、比較結果に基づいて上記復号化キー

を決定するステップとにより決定されることを特徴する請求項8に記載の復号化方法。

【請求項11】 復号化された上記特定情報と暗号化されていない上記特定情報とが一致しない場合、上記復号化キーを決定するための情報から、上記一方向関数を用いて階層化されている新たな上記復号化キーを求め、その新たな復号化キーを用いて、暗号化されている上記特定情報を復号化する動作を、復号化された上記特定情報と暗号化されていない上記特定情報とが一致するまで繰り返し、復号化された上記特定情報と暗号化されていない上記特定情報とが一致したとき、そのときの上記復号化キーを最終的な上記復号化キーとすることを特徴とする請求項10に記載の復号化方法。

【請求項12】 上記暗号化された所定の情報は、記録媒体に記録されており、その暗号化された所定の情報は、上記記録媒体から読み出されることにより供給され、

上記暗号化キーは、上記記録媒体または上記記録媒体を収納するケース上に上記暗号化キーに対応する文字、数字、バーコードもしくはホログラムとして印刷されていることを特徴する請求項6に記載の復号化方法。

【請求項13】 上記暗号化キーは、暗号化された所定の情報を復号化するための所定のソフトウェアの中に、上記暗号化キーに対応するコードとして挿入されていることを特徴とする請求項6に記載の復号化方法。

【請求項14】 上記暗号化キーは、電話回線、またはネットワークを介して供給されることを特徴する請求項6に記載の復号化方法。

【請求項15】 所定の情報を所定の暗号化キーを用いて暗号化する暗号化装置において、
一方向関数を用いて階層化することにより上記暗号化キーを発生する発生手段と、
上記階層化された暗号化キーを用いて上記所定の情報を暗号化する暗号化手段とを有することを特徴とする暗号化装置。

【請求項16】 階層化された上記暗号化キーのうち、階層化するときの最初の暗号化キーは、マスターキーであることを特徴とする請求項15に記載の暗号化装置。

【請求項17】 上記階層化された暗号化キーを用いて特定情報を暗号化する第2の暗号化手段をさらに有することを特徴とする請求項15に記載の暗号化装置。

【請求項18】 暗号化された所定の情報を復号化する復号化装置において、
暗号化された所定の情報を受信する受信手段と、
一方向関数を用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化する復号化手段とを有することを特徴とする復号化装置。

【請求項19】 上記暗号化キーに対応する復号化キーを決定するための情報を記憶する第1の記憶手段と、
一方向関数を用いてマスターキーから上記暗号化キーに

対応する復号化キーを生成する生成手段と、
上記生成された暗号化キーに対応する復号化キーを記憶する第2の記憶手段とをさらに有し、

その暗号化キーに対応する復号化キーを決定するための情報は、階層化された上記暗号化キーのうち、階層化する際の最初の暗号化キーであるマスターキーであることを特徴とする請求項18に記載の復号化装置。

【請求項20】 上記受信手段は、暗号化された特定情報を受信し、

上記生成手段は、暗号化されていない上記特定情報、暗号化されている特定情報及び上記暗号化キーに対応する復号化キーを決定するための情報から、受信した上記所定の情報を暗号化した暗号化キーに対応する復号化キーを決定し、

上記復号化手段は、その決定された復号化キーを用いて上記暗号化された所定の情報を復号化することを特徴とする請求項19に記載の復号化装置。

【請求項21】 上記暗号化キーに対応する復号化キーを決定するための上記情報は、マスターキー、もしくは最新の暗号化キーの情報であることを特徴とする請求項20に記載の復号化装置。

【請求項22】 上記生成手段は、上記暗号化キーに対応する復号化キーを決定するための上記情報を用いて上記暗号化された特定情報を復号化し、その復号化された特定情報と上記特定情報とを比較し、比較結果に基づいて暗号化キーに対応する復号化キーを決定することを特徴とする請求項21に記載の復号化装置。

【請求項23】 上記生成手段は、復号化された上記特定情報と暗号化されていない上記特定情報とが一致しない場合、上記復号化キーを決定するための情報から、上記一方関数を用いて階層化されている新たな上記復号化キーを求め、その新たな復号化キーを用いて、暗号化されている上記特定情報を復号化する動作を、復号化された上記特定情報と暗号化されていない上記特定情報とが一致するまで繰り返し、復号化された上記特定情報と暗号化されていない上記特定情報とが一致したとき、そのときの上記復号化キーを上記第2の記憶手段に記憶させることを特徴とする請求項22に記載の復号化装置。

【請求項24】 上記第1の記憶手段、上記第2の記憶手段、上記生成手段、および上記復号化手段は、1つのICチップ内に配置されていることを特徴とする請求項19に記載の復号化装置。

【請求項25】 上記暗号化キーに対応する復号化キーを決定するための情報は、予め第1の記憶手段に記憶されていることを特徴とする請求項24に記載の復号化装置。

【請求項26】 復号化装置によって復号可能な記録媒体において、
復号化装置によって復号可能な記録信号を有し、
上記記録信号は、一方関数を用いて階層化された暗号

化キーを用いて暗号化された所定の情報を含んでいることを特徴とする記録媒体。

【請求項27】 上記記録信号は、さらに、上記暗号化キーを用いて暗号化された特定情報を含んでいることを特徴とする請求項26に記載の記録媒体。

【請求項28】 上記暗号化キーは、上記記録媒体に上記暗号化キーに対応する文字、数字、バーコードもしくはホログラムとして印刷されていることを特徴とする請求項26に記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録方法によって情報が記録された記録媒体に関し、例えば、デジタル・ビデオ・ディスク（DVD）などの記録媒体に記録されたソフトウェアもしくはデータ、またはネットワークを介して供給されるソフトウェアもしくはデータ等の不正使用を防止する場合に用いて好適な暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録媒体に関する。

【0002】

【従来の技術】 通常、ソフトウェアやデータの不正使用を防止する場合、ソフトウェアやデータを所定の暗号化キーを用いて暗号化して、この暗号化されたソフトウェアまたはデータをデジタル・ビデオ・ディスク（以下、DVDと記述する）に記録したり、ネットワークを介して供給するようにしている。そして、DVDやネットワークを介して提供された暗号化されたソフトウェアまたはデータは、別途供給された上記暗号化キーを用いて復号化される。

【0003】 ここで、簡単に、情報の暗号化及び復号化について説明する。図12は、情報の暗号化及び復号化に関しての原理を示している。送り側において、平文M（送信する情報）が暗号化鍵K1を用いて暗号化ブロック101で暗号化され、暗号文C（実際に送信されるデータ）が生成される。その暗号文Cが受け側に送信され、受け側において、復号化鍵K2を用いて復号化ブロック102で復号化され、平文Mが生成される。このようにして、平文が送り側から受け側に送られる。

【0004】 また、復号化鍵を有しない者（解読者）が暗号文Cを盗聴して、その暗号文Cを解読ブロック103で解読することがある。なお、ここで、復号化鍵を有する者が復号化鍵を用いて暗号文Cから平文Mを生成することを、“復号”と呼び、復号化鍵を有しない者が暗号文Cを盗聴して暗号文Cから平文を獲得することを、“解読”と呼ぶ。

【0005】 ところで、上述したような暗号化キーを用いて暗号化を行う場合、暗号化キー一度が解読されてしまうと、以後、この暗号化キーは、不正使用の防止に対しては無効になってしまう。そこで、暗号化キーが解読

されたときには、暗号化キーを別のものに更新し、新たな暗号化キーを用いてソフトウェアまたはデータの暗号化を行うことにより、その不正使用を防止することが考えられる。

【0006】

【発明が解決しようとする課題】しかしながら、現実には、暗号化キーを更新しても、以前の暗号化キーで暗号化されたソフトウェアまたはデータが存在している場合があるので、その復号化のために以前の暗号化キーも保持しておかなければならない。このため、暗号化キーが更新される度に保持すべき暗号化キーが増加し、暗号化キーの管理がハードウェア的にも、ソフトウェア的にも容易ではなくなる課題があった。

【0007】また、ハードウェア的に暗号化キーが予め組み込まれている場合、それを新たな暗号化キーに更新すること自体が極めて困難な場合がある。

【0008】本発明は、このような状況に鑑みてなされたものであり、本発明の目的は、暗号化キーを階層化し、暗号化キーの管理を容易にする暗号化方法、暗号化装置、記録方法、復号化方法、復号化装置及び記録媒体を提供することにある。

【0009】

【課題を解決するための手段】請求項1に記載の暗号化方法は、暗号化キーを一方関数を用いて階層化し、階層化された暗号化キーを用いて所定の情報を暗号化することを特徴とする。

【0010】請求項4に記載の記録方法は、一方関数を用いて階層化された暗号化キーを用いて暗号化された所定の情報を受信し、暗号化された所定の情報を記録媒体に記録することを特徴とする。

【0011】請求項6に記載の復号化方法は、暗号化された所定の情報を受信し、一方関数を用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化することを特徴とする。

【0012】請求項15に記載の暗号化装置は、一方関数を用いて階層化することにより暗号化キーを発生する発生手段と、階層化された暗号化キーを用いて所定の情報を暗号化する暗号化手段とを有することを特徴とする。

【0013】請求項18に記載の復号化装置は、暗号化された所定の情報を受信する受信手段と、一方関数を

$$F(k) = \text{DES}(IV, k)$$

(ここで、IVは、Initial Vectorであり任意、kは鍵)

である。

【0020】また、一方関数に使うアルゴリズムとしては、例えば、以下のようなものがある。

【0021】・block cipher (product cipher) 系のアルゴリズム。

・数論的アルゴリズム。

用いて階層化された暗号化キーに対応する復号化キーを用いて暗号化された所定の情報を復号化する復号化手段とを有することを特徴とする。

【0014】請求項26に記載の記録媒体は、復号化装置によって復号可能な記録信号を有し、記録信号は、一方関数を用いて階層化された暗号化キーを用いて暗号化された所定の情報を含んでいることを特徴とする。

【0015】上記いずれの場合においても、暗号化キーとしては一方関数で階層化されたものが用いられる。

【0016】

【発明の実施の形態】図1は、本発明の暗号化方法を適用した暗号化キーの階層化の方法の例を示す図である。同図において、最初の階層の暗号化キー（マスターキー (Master key) (K0)）に対して、いわゆる一方関数F (one-way Function) を用いて、次の階層 (Ver. n) の暗号化キーK1が形成される。ここで、F はいわゆる一方関数の1つで、暗号化キーK0からK1を演算することは容易にできるが、その逆の演算、即ち、暗号化キーK1からK0を演算することは極めて困難であるような不可逆性の演算を行う関数である。

【0017】一方関数には、Data Encryption Standard (DES, National Bureau of Standards FIPS Publication 46, 1977)、Fast Encryption Algorithm (FEAL, S. Miyaguchi. The FEAL cipher family. Lecture Notes in Computer Science, 537(1001), pp627-638. (Advances in Cryptology - CRYPTO '90)) のような暗号化アルゴリズム、あるいはMessage Digest algorithm (MD4, R. L. Rivest. The MD4 message digest algorithm. Lecture Notes in Computer Science, 537(1001), 303-311. (Advances in Cryptology - CRYPTO '90)) や Secure Hash Standard (SHS, Secure Hash Standard. National Bureau of Standards FIPS Publication 180, 1993) のようなメッセージダイジェストアルゴリズムを使用することができる。なお、DES、FEALに関しては、「辻井、笠原、「暗号と情報セキュリティ」、1993年7月」に詳細に記載されている。続いて、一方関数について、例を挙げて簡単に説明する。

【0018】DESの場合、一方関数とDESとの間には、次式(1)に示すような関係がある。即ち、

【0019】

・・・(1)

【0022】block cipher (product cipher) 系のアルゴリズムは、次式(2)に示すように、平文 (Plain text) を、鍵 (key) を用いて、暗号化し、暗号文 (Cipher text) を得る。

【0023】

$C = \text{Enc}(P, k)$
 (ただし、Cはcipher text、
 Pはplain text、
 kはkey (鍵))

【0024】即ち、keyに対して、ブロック毎にある種のhash functionにより、逆戻りできないような変換を施し、固定長のビット列を得る。

【0025】次に、plain textをデータの置き換えなどを行うpermutation boxやsubstitution boxに数ラウンド通す。各

$$F(k) \leq a^k \bmod p$$

(ただし、aは所定の定数、kは鍵、pは素数)

【0028】なお、上記式(3)において、記号「 \leq 」は、「定義」を意味している。

【0029】即ち、関数F(k)を、「aをk乗したものをpで割った余り」と定義する。この場合、鍵(k)からF(k)は容易に求めることができるが、F(k)からkを求めるのは非常に困難である。

【0030】このように、一方向関数(F)を用いてマ

$$K_i = F(K_{i-1}) \quad (\text{ただし、} i = 1, 2, 3, \dots, n) \quad \dots (4)$$

【0032】なお、数値nは、十分と考えられる階層の数(世代数)である。従って、上述したように、一方向関数(F)を用いて新たに暗号化キーを演算することは容易にできるが、その逆の演算、即ち、一方向関数を用いて演算された暗号化キーから元のキーを演算することは極めて困難である。

【0033】ここで、本発明におけるソフトウェアまたはデータなどの情報を暗号化してユーザに提供する方法について説明する。ソフトウェアまたはデータ等の情報を暗号化してユーザに提供する場合、図1に示すように、最初に暗号化キー K_n (Ver. 1)を用いて情報を暗号化し、暗号化キー K_n を暗号化された情報に添付するか、もしくは別途供給するなどしてユーザに配布するようにする。ユーザは、暗号化された情報を、暗号化キー K_n を用いて復号化することができる。

【0034】そして、もし、この暗号化キー K_n が解読された場合、ソフトウェアまたはデータ等の情報を1つ上の階層(Ver. 2)の暗号化キー K_{n-1} を用いて暗号化し、暗号化キー K_{n-1} をユーザに配布するようにする。以下同様に、暗号化キーが解読される度に、解読された暗号化キーの1つ上の階層の暗号化キーを用いて情報を暗号化し、その暗号化キーをユーザに配布するようにする。

【0035】例えば、最初に配布される最下位の階層(Ver. 1)の暗号化キー K_n は、次の階層(Ver. 2)の暗号化キー K_{n-1} から関数Fを用いて演算されたものである。つまり、関数Fを用いることにより、暗号化キー K_{n-1} から暗号化キー K_n を容易に演

... (2)

ラウンドで、keyから得られたビット列とある種の演算、例えば排他的論理和演算(Exor)を施す。

【0026】また、数論的アルゴリズムは、次式(3)に示すように、離散対数問題に使用される。

【0027】

... (3)

スタキー K_0 から暗号化キー K_1 が求められた後、続いて、同様に一方向関数(F)を用いて、次式(4)に示すように、順次暗号化キー $K_2, K_3, \dots, K_{n-1}, K_n$ が演算され、階層化(Ver. n乃至Ver. 1)された暗号化キーが形成される。

【0031】

算することができ、暗号化キー K_{n-1} から演算された暗号化キー K_n を用いて、暗号化キー K_n によって暗号化された情報を復号化することができる。以下、同様に、どの世代においても、関数Fを用いることにより、次の暗号化キーを演算することができる。

【0036】従って、ユーザは、解読されていない最新の暗号化キーを保持しておくだけで、最新の暗号化キーによって暗号化された情報だけでなく、以前の暗号化キーによって暗号化された情報も復号化することができる。また、すべての暗号化キーは、一方向性関数Fを用いて、マスターキーから順次生成されるキーである。従って、ユーザは、解読されていない最新の暗号化キーの代わりにマスターキーを保持しておくだけで、すべての暗号化キーによって暗号化された情報を復号化することができる。これにより、暗号化キーの管理を容易にすることができる。

【0037】図2は、ディスクを作成する側において、図1に示した暗号化キーを用いて、例えば、ディスク(例えば、DVD)等の記録媒体に、動画、音声、データ、ソフトウェアなどの情報(平文データ: Plain text)を暗号化して記録するときの手順を説明するためのフローチャートである。最初に、ステップS1において、図1に示した階層化された暗号化キーのうち、適当な世代(階層)の暗号化キーを選択し、その選択された暗号化キーをワークキー(work key)として選択する。次に、ステップS2に進み、予め決められた所定の数字や文字の列をマジック番号(magic number)とし、そのマジック番号をステップ

S1で選択したワークキーを用いて暗号化する。そして、暗号化によって得られた暗号化されたマジック番号 (encrypted magic number) が、図3に示すように、例えば、DVD1の所定の場所に記録される。

【0038】次に、ステップS3において、隠したい情報、つまり、平文データをワークキーを用いて暗号化し、暗号化された情報 (cipher text) をDVD1の所定の場所に記録する。

【0039】次に、上述した暗号化方法に対応する暗号化装置を、図4を用いて説明する。平文データとマジック番号が、それぞれの入力端子を介して対応する暗号化回路51または52に供給される。ワークキー生成回路53は、図1に示した階層化された暗号化キーのうち、適当な世代 (階層) の暗号化キーを選択し、その選択された暗号化キーをワークキーとして、暗号化回路51、52に供給する。暗号化回路52は、供給されたマジック番号をワークキー生成回路53から供給されたワークキーを用いて暗号化する。そして、暗号化されたマジック番号が、記録装置54に供給される。

【0040】また、暗号化回路51は、供給された平文データをワークキーを用いて暗号化し、暗号化された情報を記録装置54に供給する。そして、記録装置54は、暗号された情報及び暗号化されたマジック情報を、図3に示すように、例えば、DVD1の所定の場所に記録する。なお、この記録装置54がマスターディスクを生成するフォーマットである場合には、その原盤からスタンパが形成され、その後、そのスタンパを使って、大量のディスクが生産される。

【0041】図5は、上述したようにして作成されたDVD1を再生するディスクプレーヤー (DVDプレーヤー) において、DVD1に記録された暗号化された情報の復号化を行うICチップの構成例を示すブロック図である。ICチップ11には、マジック番号 (magic number)、暗号化されたマジック番号 (encrypted magic number) および暗号化された情報 (cipher text) が入力されるようになっている。暗号化されたマジック番号としては、DVD1から再生されたものが供給され、マジック番号としては、DVDプレーヤー自身が図示せぬメモリなどに保持していたものが、そのメモリから読み出されて供給される。このマジック番号は、予め決められた所定の数字や文字の列であり、暗号化側で使用されたマジック番号と同一のものである。

【0042】メモリ12は、図1に示した暗号化キーK0、即ち、マスターキーを保持するようになっている。レジスタ13は、後述するようにして、マスターキーに対して上記関数Fを用いて求められた所定の世代の暗号化キー、即ちワークキー (work key) を保持するようになっている。復号化回路14は、後述す

るように、まず、入力されたマジック番号、暗号化されたマジック番号およびメモリ12から読み出されたマスターキーに基づいて、ワークキーを作成し、その作成されたワークキーをレジスタ13に供給するようになっている。そして、復号化回路14は、入力された暗号化された情報 (Cipher Text) をワークキーを用いて復号化し、平文データ (Plain text) として出力するようになっている。

【0043】次に、図6に示したフローチャートを参照して、ICチップ11内におけるDVD1に記録された暗号化された情報を復号化する手順について説明する。最初に、ステップS11において、DVD1の所定の場所に記録された暗号化されたマジック番号が読み出される。次に、ステップS12に進み、ステップS11において読み出された暗号化されたマジック番号と、DVDプレーヤー自身が有する図示しないメモリから読み出されたマジック番号から、図7のフローチャートを参照して後述するようにしてワークキーを求める。

【0044】図7は、図6のステップS12における処理の詳細を説明するためのフローチャートである。最初に、ステップS21において、ICチップ11のメモリ12よりマスターキーが読み出され、これが選択キー (k) とされる。そして、この選択キー (k) が、復号化回路14に供給される。ここで、選択キー (k) は、現在選択されている暗号化キーを表すものとする。

【0045】次に、ステップS22に進み、復号化回路14は、供給された、暗号化されているマジック番号 (MNe) を選択キー (k) を用いて復号化する。そして、暗号化されているマジック番号を選択キー (k) で復号化した結果とマジック番号とが一致するか否かを判定する。復号化した結果と暗号化されていないマジック番号とが一致しないと判定された場合、この選択キーは、暗号化側において、暗号化されたマジック番号を暗号化した暗号化キーではないと判定される。よって、ステップS23に進み、次式 (5) に示すように、選択キー (k) から一方向関数 (F) を用いて、次の世代の暗号化キーを演算し、それを新たに選択キー (k) とする。

$$【0046】k = F(k) \cdots (5)$$

【0047】そして、再び、ステップS22に戻り、上述した場合と同様の処理を繰り返し実行する。

【0048】一方、ステップS22において、暗号化されているマジック番号を選択キー (k) で復号化した結果と、暗号化されていないマジック番号が一致すると判定された場合、選択キー (k) は、暗号化側において、暗号化されたマジック番号を暗号化した暗号化キーであると判定される。よって、ステップS24に進み、復号化回路14は、この選択キー (k) をワークキーとし、それをレジスタ13に供給し、レジスタ13に記憶させる。そして、この図7のフローチャートの処理が終了さ

れ、図6のフローチャートの処理に戻る。

【0049】その後、図6のフローチャートのステップS13に進み、復号化回路14は、ステップS12（図7のステップS21乃至24）において求められたワークキーをレジスタ13から読み出し、入力された暗号化されている情報（Cipher Text）を、ワークキーを用いて復号化し、平文データ（Plain Text）として出力する。

【0050】このように、ICチップ11は、マスターキーから、暗号化された情報に対応するワークキーを求め、入力された暗号化された情報をこのワークキーを用いて復号化するので、マスターキーを保持しておくだけで、任意の階層の暗号化キーによって暗号化された情報を復号化することができる。

【0051】上述したような処理を、コンピュータのソフトウェアによって行う場合、図6のステップS12の処理は、図8に示したようになる。即ち、図8は、図5に示したような機能をソフトウェアで実現するコンピュータにおいて、暗号化された情報が復号化される手順を示すフローチャートである。この場合、コンピュータは、図5に対応するような復号基板を内蔵しており、その基板のメモリにソフトウェアが記憶されている。また、この場合、予めメモリに記憶されているマスターキーを使用するのではなく、配布される最新の暗号化キー（マスターキーの場合もある）を使用する。

【0052】例えば、図9を参照して後述するように、DVDに印刷されて配布された所定の階層の暗号化キー（ K_i ）（ここで、 i は n 、 $n-1$ 、 \dots 、1のいずれか）をユーザがキーボードを介してコンピュータに入力する。その暗号化キーが、コンピュータ内の所定のメモリに記憶されるようになされている。あるいは、コンピュータは、電話回線やネットワークを介して配布された最新の暗号化キーを受信し、それを所定のメモリ（例えば、RAM）に記憶するようになされている。

【0053】最初に、ステップS31において、入力された所定の階層の暗号化キー（ K_i ）がメモリから読み出され、選択キー（ k ）とされる。ここで、選択キー（ k ）は、上述した場合と同様に、現在選択されている暗号化キーを表すものとする。

【0054】次に、ステップS32に進み、暗号化されているマジック番号が選択キー（ k ）を用いて復号化される。そして、暗号化されているマジック番号を選択キー（ k ）で復号化した結果とマジック番号とが一致するか否かが判定される。復号化した結果と暗号化されていないマジック番号とが一致しないと判定された場合、選択キー（ k ）は、暗号化側において、マジック番号を暗号化した暗号化キーではないと判定される。よって、ステップS33に進み、上記式（5）に示したように、選択キー（ k ）から一方関数（ F ）を用いて、次の世代の暗号化キーを演算し、それを新たに選択キー（ k ）と

する。

【0055】そして、再び、ステップS32に戻り、上述した場合と同様の処理を繰り返し実行する。

【0056】一方、ステップS32において、暗号化されているマジック番号を選択キー（ k ）で復号化した結果とマジック番号とが一致すると判定された場合、選択キー（ k ）は、暗号化側において、マジック番号を暗号化した暗号化キーであると判定される。よって、ステップS34に進み、この選択キー（ k ）をワークキーとし、このワークキーが所定のメモリ（例えば、レジスタ）に記憶される。そして、この図8のフローチャートの処理が終了され、図6のフローチャートの処理に戻る。

【0057】その後は、図6のフローチャートのステップS13に進み、ステップS12（図8のステップS31乃至S34）において求められたワークキーを用いて、暗号化された情報を復号化し、平文データ（Plain Text）として出力する。

【0058】このように、暗号化されている情報の復号化を、コンピュータのソフトウェアで行う場合においては、配布された任意の階層の暗号化キーに基づいて、少なくともその暗号化キー（ K_i ）、またはその暗号化キーの階層よりも低い階層の暗号化キー（ K_{i-1} 乃至 K_1 ）によって暗号化されている情報を復号化することができる。

【0059】このように、本発明の実施の形態においては、最新の暗号化キー（マスターキーの場合も有り得るし、任意の階層の暗号化キーの場合も有り得る）に基づいて、それ以前の暗号化キーによって暗号化された情報をも復号化することができるので、最新の暗号化キーだけを記憶しておけばよく、従来のように、暗号化キーが解読され、暗号化キーが変更される度に、それ以前の暗号化キーに加えて新たな暗号化キーを記憶し、管理する必要がなくなり、暗号化キーの管理を容易にすることができる。

【0060】また、図5の実施の形態においては、暗号化キー（マスターキー）を、チップ11のメモリ12に記憶させ、そのチップ内で所定の階層の暗号化キーを演算し、暗号化された情報を復号化するようにしたので、暗号化キーが外部に漏れることを抑制することができ、暗号化キーの解読を困難にすることができる。さらに、上記実施の形態においては、ワークキーの算出処理と、暗号化された情報の復号化処理とを同一の復号化回路14で行うようにしたので、構成を簡略化することができる。

【0061】次に、図9乃至図11を参照して、暗号化キーを配布する方法について説明する。

【0062】図9は、暗号化キーをDVDのケースやDVD自体に印刷して配布する例を示している。

【0063】例えば、所定の階層の暗号化キーAに対応するアルファベット文字、数字、バーコード、あるいは

ホログラム等を、タイトルAが記録されたDVD 2 1のケースやDVD 2 1自体の表面等に印刷する。同様に、所定の階層の暗号化キーBに対応するアルファベット文字、数字、バーコード、あるいはホログラム等を、タイトルBが記録されたDVD 2 2のケースやDVD 2 2自体の表面等に印刷する。このようにして、暗号化キーAをDVD 2 1とともに、また、暗号化キーBをDVD 2 2とともに、ユーザに配布することができる。

【0064】あるいは、ICカード等の記録媒体に暗号化キーAを表すデータを記録してDVD 2 1とともに、また、ICカード等の記録媒体に暗号化キーBを表すデータを記録してDVD 2 2とともに配布するようにすることも可能である。

【0065】ユーザは、DVD 2 1を再生する場合、DVD 2 1に印刷された暗号化キーAを、コンピュータ2 3にキーボード等の入力装置2 4を用いて入力する。コンピュータ2 3は、図8のフローチャートを参照して、上述したように、例えば、図5に示したICチップ1 1が行う機能、即ち暗号化された情報を復号化する機能を所定のアプリケーションプログラムによって実行するようになされている。

【0066】次に、DVD 2 1を図示せぬDVD読み取り装置にセットすると、コンピュータ2 3は、DVD読み取り装置を介して、DVD 2 1から暗号化された情報を読み出し、先に入力された暗号化キーAに基づいて、DVD 2 1から読み出した暗号化されている情報を復号化する。DVD 2 2についてもDVD 2 1の場合と同様に、そこに記録された暗号化されている情報を復号化することができる。

【0067】従って、この例は、DVDのタイトル毎に異なる暗号化キーを配布する場合、例えば、DVDのタイトル毎に、異なるマスタキーから一方向関数によって演算された暗号化キーを割り当てるような場合に適している。

【0068】例えば、タイトルAに対応する暗号化キーAが解読され、タイトルAに対応する暗号化キーAが、その上の階層の暗号化キーA2に更新され、タイトルAの続編が暗号化キーA2によって暗号化されている場合でも、更新される前の暗号化キーAは、図8を参照して上述したように、暗号化キーA2から所定の演算によって容易に求めることができる。従って、ユーザは、最新の暗号化キー（この場合、暗号化キーA2）だけを用いて、以前の暗号化キーで暗号化されたタイトルAをも復号化することができる。

【0069】図10は、暗号化キーを復号化するためのソフトウェアに、暗号化キーを表すコードを挿入して配布する例を示している。

【0070】即ち、暗号化情報を復号化する復号化基板3 3に設けられている復号化のためのソフトウェアの中に、暗号化キーを表すコードが挿入される。そして、こ

の復号化基板3 3をコンピュータ2 3に装着する。これにより、コンピュータ2 3は、DVD 3 1、3 2に記録された暗号化された情報を復号化基板3 3を介して復号化することができ、復号化した情報に対応する動画、静止画、および音声などを出力することができる。

【0071】この例は、DVDのタイトルに依らず、同一の暗号化キーを配布する場合に適している。

【0072】また、この例の場合、コンピュータ2 3を電話回線あるいはネットワークに接続し、更新した暗号化キーを電話回線あるいはネットワークを通じてコンピュータ2 3に配布するようにすることも可能である。コンピュータ2 3は、電話回線またはネットワークを介して配布された最新の暗号化キーを、復号化基板3 3の復号化のためのソフトウェアの中に記憶させる。

【0073】そして、コンピュータ2 3は、この暗号化キーを用いて、図6および図8を参照して上述したようにして、DVD 3 1、3 2に記録された情報を復号化することができる。

【0074】また、電話回線またはネットワークを介して暗号化キーによって暗号化した情報を伝送し、コンピュータ2 3に提供するようにすることができる。この場合、コンピュータ2 3は、先に電話回線またはネットワークを介して配布された暗号化キーを用いてこの情報を復号化する。

【0075】ところで、図1を参照して上述したように、階層化した最初の暗号化キー（K0）から、一方向関数（F）を用いて全ての階層の暗号化キーを形成することができ、この暗号化キーK0をマスタキーとすることができる。そこで、このマスタキーとなる暗号化キーK0を、集積回路等のハードウェアの中に埋め込んでおくことにより、この暗号化キーK0から全ての階層の暗号化キーを作成することができ、どの暗号化キー（K1乃至Kn）で暗号化された情報でも復号化することができるようにすることができる。通常のユーザにとって、集積回路等のハードウェアに埋め込まれたデータを解読することは困難であるので、このようにして暗号化キーの不正使用を抑制することができる。

【0076】図11は、このように集積回路に暗号化キーを埋め込んで配布する例を示している。同図において、所定の守秘義務を有する製造者によって、マスタキーを記憶する集積回路4 1が製造される。この集積回路4 1には、例えば、図5に示したICチップ1 1を適用することができる。そして、この例の場合、この集積回路4 1が製造者Aに供給され、製造者AによってDVDプレーヤ4 3に組み込まれた後、ユーザに提供される。

【0077】一方、DVD 4 2には、集積回路4 1が記憶する所定の階層の暗号化キーを用いて暗号化されたマジック番号、およびこの暗号化キーを用いて暗号化された所定の暗号化情報が記録される。

【0078】ユーザが、DVD 4 2をDVDプレーヤ4

3にセットすると、集積回路41からマスタキーが読み出され、図6および図7のフローチャートを参照して上述したようにして、ワークキーが求められ、DVD42に記録された暗号化された情報が復号化され、対応する動画、静止画、および音声が出力される。

【0079】このように、集積回路41にマスタキーを記憶させた場合、DVDプレーヤ43は、DVD42に記録された情報がどの階層の暗号化キーによって暗号化されていたとしても、DVD42に記録された暗号化された情報を復号化して出力させることができる。

【0080】また、集積回路41にマスタキーではなく、マスタキーから一方関数を用いて演算される暗号化キーのうちの所定の階層の暗号化キーを記憶させることもできる。その場合、その暗号化キーまたはその暗号化キーより低い階層の暗号化キーによって暗号化された情報がDVD42に記録されているとき、DVDプレーヤ43は、DVD42に記録されたその情報を復号化することができる。

【0081】このように、所定の集積回路に所定の暗号化キーを記憶させ、それをDVDプレーヤ43に組み込む方法は、DVDのタイトルに依らず同一の暗号化キーを配布する場合に適している。

【0082】以上のように、暗号化キーを一方関数を用いて階層化し、階層化した暗号化キーのうち、任意の階層の暗号化キーを用いて情報を暗号化するとともに、この暗号化キーをユーザに配布することにより、ユーザは最新の暗号化キーを保持するだけで、以前の暗号化キーによって暗号化された情報も復号化することができる。これにより、暗号化キーを容易に管理することができる。

【0083】例えば、図11に示した実施の形態は、特に、ネットワーク等を介して暗号化キーのやりとりを容易に行うことができないような場合に、より有効に適用することができる。即ち、DVD42にソフトウェアや動画等の情報が所定の階層の暗号化キーによって暗号化されて記録されている場合において、集積回路41はマスタキーを記憶しているので、このマスタキーから一方関数(F)を用いて任意の階層の暗号化キーを作成することができ、DVD42に記録されている所定の階層の暗号化キーによって暗号化された情報を復号化することができる。

【0084】これにより、ユーザは、暗号化キーが解読されるなどして更新され、DVD42に新たな階層の暗号化キーによって暗号化された情報が記録されたとしても、従来通り特に意識することなくそれを復号化して再生することができる。

【0085】また、暗号化キーを記憶する集積回路41を有していないDVDプレーヤにおいては、この暗号化キーによって暗号化された情報が記録されたDVD42を正しく再生することができないので、情報の利用を

適切に制限することができる。同様に、暗号化キーを記憶する復号基板を有していないコンピュータにおいては、この暗号化キーによって暗号化された情報が記録された記録媒体を正しく再生することができないので、情報の利用を適切に制限することができる。

【0086】さらに、DVDなどの記録媒体またはそのケースに暗号化キーを表すアルファベット文字、数字、バーコード、あるいはホログラム等を印刷したり、ICカードに暗号化キーに対応するデータを記憶させたり、不正使用が困難な集積回路内に暗号化キー（例えば、マスタキー）に対応するデータを記憶させたり、復号化のためのソフトウェアの中に暗号化キーに対応するデータを挿入したり、あるいは電話回線やネットワークを介して伝送するなどして、極めて容易に暗号化キーを配布することができる。

【0087】なお、上記実施の形態においては、記録媒体としてDVDを用いるようにしたが、勿論これに限定されるものではなく、CD-ROM、MD（ミニディスク）（商標）、光ディスク、光磁気ディスク、またはフロッピーディスク等のその他の記録媒体を用いるようにすることも可能である。

【0088】また、本発明は、インターネット等のネットワークを介して、情報を提供する場合にも適用することが可能である。

【0089】さらに、上記実施の形態においては、マジック番号をDVDプレーヤ自身が所定のメモリ等に保持するようにしたが、例えば、DVDの所定の場所に記録し、それを読み出して復号化回路14に入力させるようにすることも可能である。その場合、図4に示すように、マジック番号が記録装置54に供給されて、ディスク1に記録される。また、コンピュータにおいて、暗号化されている情報をソフトウェアによって復号化するようになされているが、ソフトウェアを使用せずに、ICチップをコンピュータに内蔵して、ICチップに復号動作を行わせるようにしてもよい。この場合、暗号化キーを記憶する集積回路41を有していないコンピュータは、暗号化された情報を正しく復号化することができないので、情報の利用を適切に制限することができる。

【0090】なお、本発明の主旨を逸脱しない範囲において、さまざまな変形や応用例が考えうる。従って、本発明の要旨は、実施の形態に限定されるものではない。

【0091】

【発明の効果】以上のごとく、請求項1に記載の暗号化方法、請求項4に記載の記録方法、請求項15に記載の暗号化装置、および請求項26に記載の記録媒体によれば、暗号化キーを一方関数を用いて階層化するようにしたので、復号化側において、最新の暗号化キーを保持するだけで、古い暗号化キーで暗号化された情報をも復号化することができ、暗号化キーが更新された場合における暗号化キーの世代管理を容易にすることが可能とな

る。

【0092】また、請求項6に記載の復号化方法、および請求項18に記載の復号化装置によれば、一方向関数を用いて階層化された暗号化キーを用いて復号化を行うようにしたので、最新の暗号化キーを保持するだけで、古い暗号化キーで暗号化された情報をも復号化することができる。

【図面の簡単な説明】

【図1】本発明の暗号化方法に適用される暗号化キーの階層構造の例を示す図である。

【図2】暗号化した情報を記録したDVDを作成する手順を示すフローチャートである。

【図3】暗号化されたマジックキーと暗号化された情報が記録されたDVDを示す図である。

【図4】本発明における暗号化装置の構成例を示すブロック図である。

【図5】図3のDVDに記録された情報を復号化するチップ11の構成例を示すブロック図である。

【図6】図5のチップ11の動作を説明するためのフロ

ーチャートである。

【図7】図6のステップS12の詳細を説明するためのフローチャートである。

【図8】図6のステップS12の詳細を説明するための他のフローチャートである。

【図9】暗号化キーをDVDに印刷して配布する方法を説明するための図である。

【図10】暗号化キーを復号化のためのソフトウェアに挿入して配布する方法を説明するための図である。

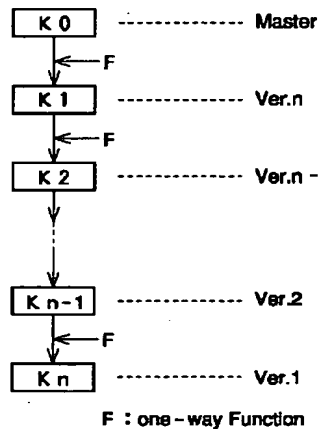
【図11】集積回路に暗号化キーを埋め込んで配布する方法を説明するための図である。

【図12】暗号化及び復号化の原理を示す図である。

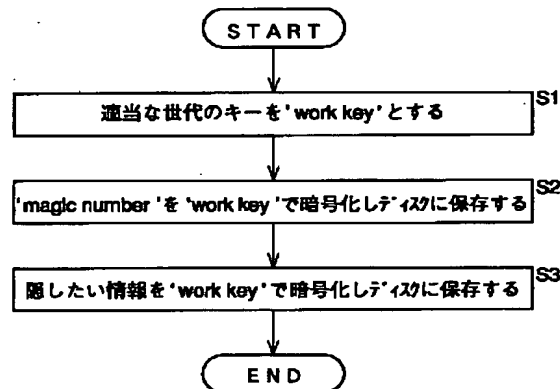
【符号の説明】

1 ディスク, 11 チップ, 12 メモリ, 13 レジスタ, 14 復号化回路, 21, 22 DVD, 23 コンピュータ, 31, 32 DVD, 33 復号化基板, 41 集積回路, 42 DVD, 43 DVDプレーヤ

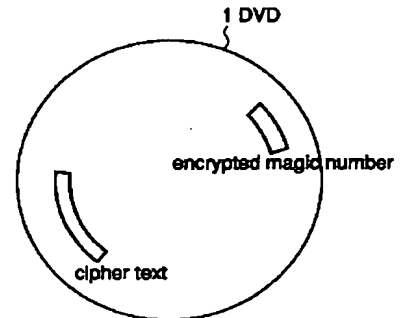
【図1】



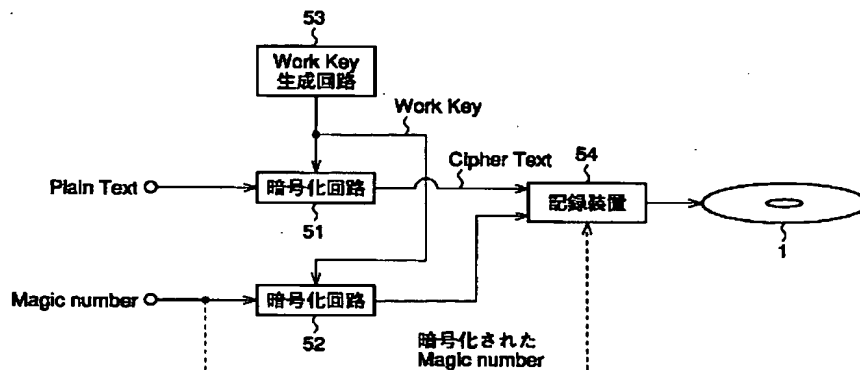
【図2】



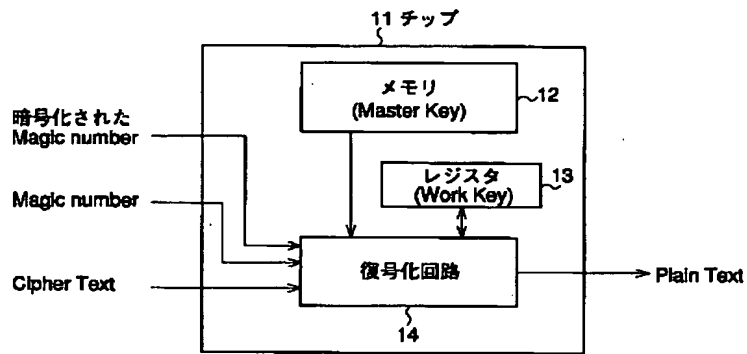
【図3】



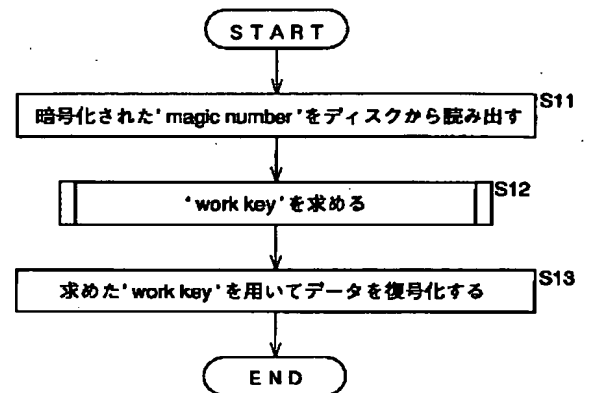
【図4】



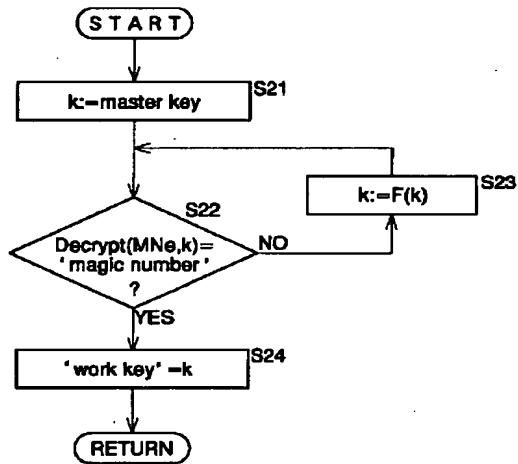
【図5】



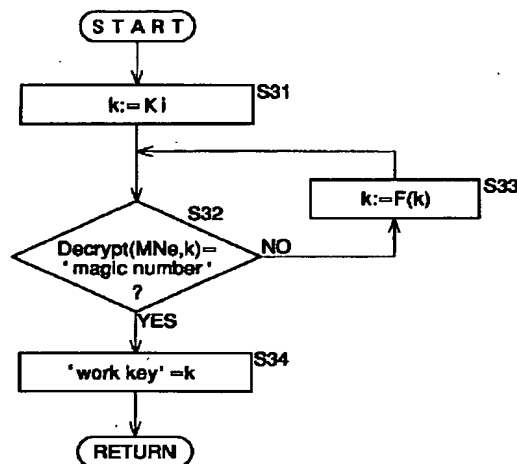
【図6】



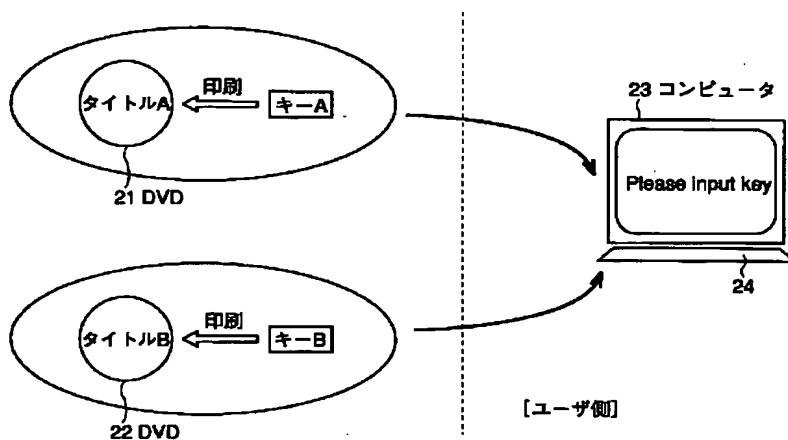
【図7】



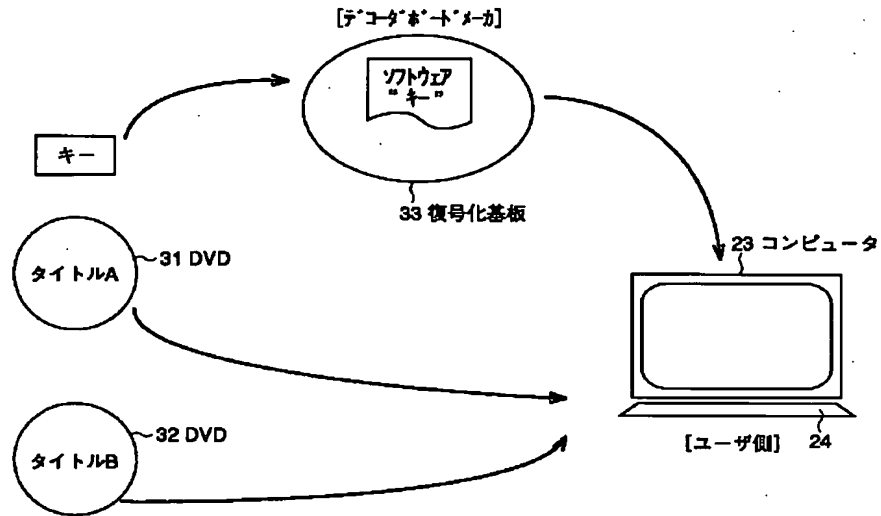
【図8】



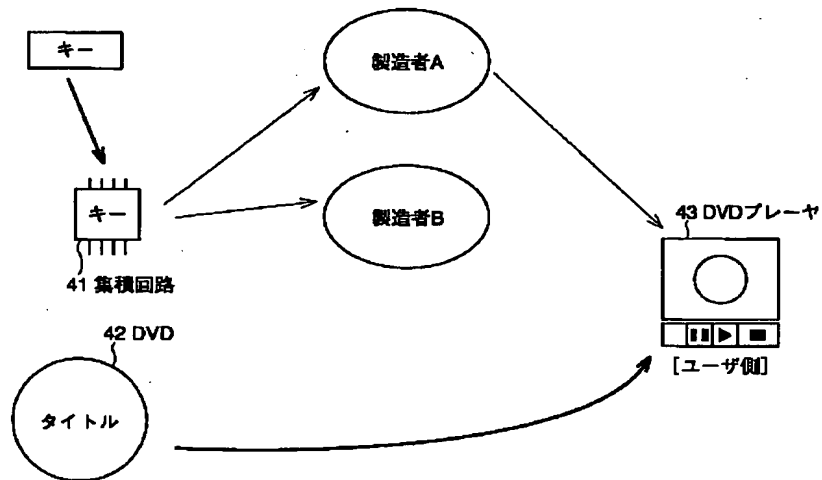
【図9】



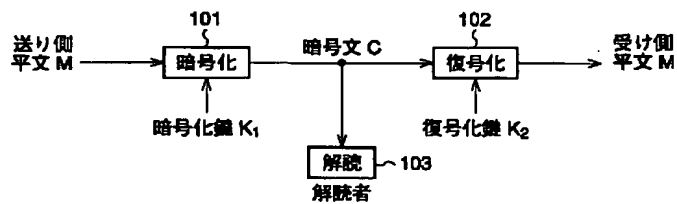
【図10】



【図11】



【図12】



フロントページの続き

(51) Int. Cl. 6

H 0 4 L 9/08

9/06

識別記号

庁内整理番号

F I

H 0 4 L 9/00

技術表示箇所

6 0 1 A

6 1 1 A

